UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

records and other information, including the contents of communications, associated with the Apple ID associated with "kwesensandersb2r@icloud.com" that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA.

Case No. 23 MJ 187

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922(g)(1)	Felon in Possession of a Firearm
18 U.S.C. § 924(c)	Possession of a Firearm in furtherance of a Federal Drug Trafficking Crime
21 U.S.C. §§ 841(a)(1) and 84	Distributing and Conspiracy to Distribute a Controlled Substance

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

NDIVA MALAFA (Affiliate) Digitally signed by NDIVA MALAFA (Affiliate) Date: 2023.11.06 19:13:19 -06'00'

Applicant's signature

Ndiva Malafa, Task Force Officer, ATF

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 11/8/2023

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ndiva Malafa, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with the Apple ID associated with "kwesensandersb2r@icloud.com" that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Task Force Officer (TFO) of the United States Justice Department, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), currently assigned to the Milwaukee Field Office. I have been so employed, as a law enforcement officer, with the Milwaukee Police Department since December 2014. I have been assigned to the ATF Task Force since February 2022. My duties with ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

3. I completed approximately 26 weeks of basic training at the Milwaukee Police Departments Training Academy (Milwaukee, WI) and a three-day ATF Task Force Officer orientation/training at ATF's Headquarters (Washington DC). The training included courses related to constitutional law and search and seizure. I also received training on conducting criminal investigations, including interviews, surveillance, and evidence collection.

4. My most recent position is with the Milwaukee Police Department in Milwaukee, Wisconsin, where I am a Patrol Officer assigned to the Criminal Investigations Bureau – Special Investigations Division as a TFO with the ATF.

5. During my career as a Police Officer, I have attended additional training in areas including firearm investigation, gang investigations, and drug investigations.

6. The information below is known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during their official duties and whom I consider to be truthful and reliable.

7. I submit this affidavit for the limited purpose of demonstrating sufficient probable cause for the requested warrant. It does not set forth all of my knowledge about this matter.

8. Based on the circumstances described below, there is probable cause to believe that on or about August 8th, 2023, Kwesen L. Sanders, DOB XX/XX/1995, has committed firearm and controlled substances offenses in the Eastern District of Wisconsin, in violation of Title 18, United States Code, Sections 922(g)(1) and 924(a)(8) (felon in possession of a firearm) and 924(c) (use of a firearm during drug trafficking), and Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(C) (possession with intent to distribute controlled substances), and that the items described in Attachment A contain evidence of those crimes.

PROBABLE CAUSE

August 8, 2023 – Fleeing and Firearms Offense

9. On August 8th, 2023, officers with the Milwaukee Police Department (MPD) observed a black 2021 Honda Civic, bearing WI registration plate ATA-8493, with illegal window tint. MPD officers were able to observe the driver, through the front windshield, as

black male, late 20's, dark complexion, with golden grill in his teeth. Eventually, officers identified the driver as Kwesen L. SANDERS, black male, DOB XX/XX/1995.

10. Once in the area of South 22nd Street and West Greenfield Avenue, officers observed SANDERS operating the Honda Civic at a high rate of speed, in an attempt to evade law enforcement detection. Officers then attempted to conduct a traffic stop of the Honda Civic by activating their emergency lights and sirens. SANDERS, who was the sole occupant and driver of the Honda Civic, disregarded the officer's emergency lights and sirens and proceeded to flee at a high rate of speed, initiating a vehicle pursuit. During the pursuit, SANDERS operated at least twice over the posted speed limit with his vehicle lights extinguished. This created a substantial risk for collision with other vehicles and pedestrians, thus showing an utter disregard for human life and safety.

11. The pursuit concluded in the 2600 block of West Highland Boulevard, Milwaukee, WI, with a total distance of 2.20 miles. At the conclusion of the pursuit, SANDERS egressed from the driver's seat of the Honda Civic and fled on foot from uniformed MPD officers. Officers were unable to locate SANDERS.

12. MPD officers responded back to the abandoned Honda Civic and conducted a search of the vehicle. The following items were recovered:

a. A black Glock-19 9mm handgun with a rear Machine Gun Conversion Device (Glock Switch), and 31-round extended-capacity magazine;

b. A knotted sandwich baggie containing a white chunky substance which was suspected cocaine, located inside a black backpack on the driver floorboard;

c. A knotted sandwich baggie containing an orange chunky substance which was suspected methamphetamines, located inside a black backpack on the driver floorboard;

d. A knotted sandwich baggie containing a dark gray chunky substance which was suspected heroin, located inside a black backpack on the driver floorboard;

e. A knotted sandwich baggie containing six (6) individual corner cut baggies of a dark gray chunky substance which was suspected heroin, located inside a black backpack on the driver floorboard;

f. A digital scale located inside a black backpack on the driver floorboard;

g. A Wisconsin Driver's License addressed to SANDERS, located in the center console;

h. A Vehicle Services Division paperwork addressed to SANDERS, located in the center console;

i. A pay stub from Crossroads Care Center of Pewaukee addressed to SANDERS, located in the center console;

j. Two cell phones located between the driver's seat and center console, further described as a red Apple iPhone (MPD Inventory #23025777, Item #2) and a blue Apple iPhone (MPD Inventory #23025777, Item #3).

13. Law enforcement tested the suspected cocaine to the Nark II#7 test and received a positive result for cocaine with a total weight of 3.92 grams.

14. The suspected methamphetamines were tested using the Nark II#01/15 and tested positive for methamphetamine with a total weight of 6.02 grams.

15. The suspected heroin was tested using the Nark II#11 and tested positive for opiates and fentanyl with a total weight of 2.7 grams.

16. The suspected heroin was tested using the Nark II#11 and tested positive for opiates and fentanyl with total weight of 1.23 grams.

17. Officers conducted a Wisconsin Department of Transportation search of the Honda Civics registration plate (ATA-8493). This search revealed the vehicle's registered owner was SANDERS.

18. Based on the weight of the drugs, the packaging, the presence of a firearm, multiple cell phones, and a digital scale, it appears the controlled substances were for distribution and not personal use.

19. ATF Milwaukee became aware of the details of SANDERS's arrest and the device's existence and location on August 24th, 2023. Shortly thereafter, a search warrant was drafted and executed on the two cellular devices, as described in paragraph 4.

20. Pursuant the aforementioned search warrant, TFO Malafa analyzed the recovered data retrieved from the cellular devices. The examination showed that the Apple ID assigned to the cell phone was iCloud account of "kwesensandersb2r@icloud.com".

INFORMATION REGARDING APPLE ID AND iCLOUD[1]

21. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

22. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

23. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

24. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address.

Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

25. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

26. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

27. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP

address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

28. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on

iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

29. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

30. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

31. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access

the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

32. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

33. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

34. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B,

government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant.

37. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

38. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with **kwesensandersb2r@icloud.com** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

c. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

d. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

e. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

f. All records pertaining to the types of service used;

g. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. **Information to be seized by the government**

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 922(g)(2) and 924(a)(8) (felon in possession of a firearm); 924(c) (use of a firearm during drug trafficking crime) – and Title 21, United States Code, Sections 841(a)(1) and 841 (b)(1)(c) (possession with intent to distribute controlled substances) involving SANDERS since August 8th, 2023, including, for the account listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation;

e. Evidence of vehicles the subscriber has used;

f. Evidence of the subscriber's possession and use of firearms;

g. Any photographs depicting the subscriber's clothing and/or hairstyle during the time period identified above;

h. Evidence of communications between the subscriber and his co-conspirators or aiders and abettors;

i. Evidence of the execution of the subscriber's criminal activity, including but not limited to, records of his travel during the above time period; and

j. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.